

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

THOMAS LUCA JR., individually and on behalf of
all others similarly situated,

Plaintiff,

v.

WYNDHAM WORLDWIDE CORPORATION,
WYNDHAM HOTEL GROUP, LLC, WYNDHAM
HOTELS AND RESORTS, LLC, and WYNDHAM
HOTEL MANAGEMENT, INC.,

Defendants.

Civil No. 2:16-cv-00746 (MRH)

Electronically Filed and Served

**[PROPOSED] STIPULATED ORDER RE:
DISCOVERY OF ELECTRONICALLY STORED INFORMATION**

1. PURPOSE

This Order will govern discovery of electronically stored information ("ESI") (including scanned hard-copy documents) in this case as a supplement to the Federal Rules of Civil Procedure, this Court's Guidelines for the Discovery of Electronically Stored Information, and any other applicable orders and rules.

2. COOPERATION

The parties are aware of the importance the Court places on cooperation and commit to cooperate in good faith throughout the matter consistent with this Court's Guidelines for the Discovery of ESI.

3. RESOURCE PERSON

The parties do not plan to utilize a resource person.

4. PRESERVATION

To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:

- a. ESI relating to the above-captioned matter will be preserved to the extent that it existed as of June 2016.

- b. In terms of preservation, the parties agree that there is no need for forensic images of servers, databases, computers, cell phones, or other electronic devices.

5. SEARCH AND IDENTIFICATION

The parties agree that in responding to an initial Fed. R. Civ. P. 34 request, or earlier if appropriate, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production in discovery and filter out ESI that is likely not subject to discovery. In an effort to limit the burdens and costs imposed by discovery in this matter, the parties are permitted to use reasonable search methods to narrow down the ESI to be reviewed for production in discovery (e.g., search terms, technology assisted review, deduplication, elimination of correspondence with attorneys, client self-collection efforts, etc.).

6. PRODUCTION FORMATS

The parties agree to produce ESI in a format consistent with Appendix 1 of this Order.

7. ESI PROTECTED FROM DISCOVERY OR PUBLIC DISCLOSURE

- a. The parties have entered into a separate agreement regarding the inadvertent disclosure of privileged information.
- b. The parties have entered into a separate agreement regarding the designation of confidential information that may be exchanged during discovery.
- c. The parties have agreed that communications involving outside and in-house counsel that post-date the filing of the complaint need not be placed on a privilege log.
- d. The parties have agreed that documents and communications may be identified on a privilege log by category, rather than individually.

8. MODIFICATION

This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

IT IS SO STIPULATED, through Counsel of Record.

Dated:

Counsel for Plaintiff

Dated:

Counsel for Defendant

IT IS SO ORDERED that the foregoing Agreement is approved.

Dated:

UNITED STATES DISTRICT/MAGISTRATE JUDGE

APPENDIX 1
PRODUCTION FORMAT AND METADATA

1. **Production Components.** Except as otherwise provided in this Stipulation and Appendix, productions of hardcopy documents and electronically stored information shall be in the following format: single page TIFFs, searchable Text Files, an ASCII delimited searchable metadata file (.dat tile) and an image load file that can be loaded into commercially acceptable production software (e.g., Relativity).

2. **TIFFs.** Documents and electronically stored information should be produced as single-page, black and white, group IV TIFFs imaged at 300 dpi. The document's original orientation should be maintained (i.e., portrait to portrait and landscape to landscape). Bates numbers, confidentiality designations (in accordance with the Confidentiality Order governing the case), and redactions (to the extent they are necessary) should be burned into the image. TIFF image tiles should be provided in an "Images" folder.

3. **Unitizing Hardcopy Documents.** In scanning paper documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records. In the case of an organized compilation of separate hardcopy documents - for example, a binder containing several separate documents behind numbered tabs - the document behind each tab should be scanned separately, but the relationship among the documents in the binder should be reflected in proper coding of the family fields as described in this Stipulation. The parties will undertake reasonable efforts to, or have their vendors, unitize documents correctly, and will commit to address situations of improperly unitized documents.

4. **OCR.** To the extent that hard copy documents have been run through optical character recognition ("OCR") software, the full text shall be provided on a document-level in an appropriately formatted text tile (.txt) that is named to match the first Bates number of the

document. OCR shall be provided for all electronic documents as full extracted text on a document-level in an appropriately formatted text file (.txt) that is named to match the first Bates number of the document. Text files should be provided in a “Text” folder. To the extent that a document is redacted, the text files should not contain the text of the redacted portions.

5. **Unique IDs.** Each TIFF image should have a unique filename, which corresponds to the Bates number of that page. The filename should not contain any blank spaces and should be padded to 8 digits, taking into consideration the estimated number of pages to be produced. If a Bates number or set of Bates numbers is skipped in a production, the producing party will so note in a cover letter or production log accompanying the production.

6. **Data Load Files.** Documents and electronically stored information should be provided with an Opticon Cross-Reference File and Concordance data load file using standard Concordance delimiters:

- (i) Field Separator: ASCII character 20 (“,”);
- (ii) Quote: ASCII character 254 (“p”); and
- (iii) New Line: ASCII character 174 (“®”).

Concordance-compatible image and data load files should be provided in a “Data” folder.

7. **Metadata.** Paragraph 10 of this Appendix sets forth the minimum metadata fields that must be produced to the extent that metadata exists for a particular document or electronically stored information. To the extent that metadata does not exist, is not reasonably accessible or available, or would be unduly burdensome to collect, nothing in this ESI Protocol shall require any party to extract, capture, collect or produce such data except for those fields specially identified in Paragraph 10 immediately preceding the table in Paragraph 10.

8. **Image Load File.** Shall contain the following comma-delimited fields: BEGBATES, VOLUME, IMAGE FILE PATH, DOCUMENT BREAK, FOLDER BREAK, BOX BREAK, PAGE COUNT.

9. **Production of ESI.** TIFFs. Electronically stored information should be produced as single-page, black and white, group IV TIFFs imaged at 300 dpi. The document's original orientation should be maintained (i.e., portrait to portrait and landscape to landscape). Bates numbers, confidentiality designations (in accordance with the Confidentiality Order governing the case), and redactions (to the extent they are necessary) should be burned into the image. TIFF image files should be provided in an "Images" folder.

10. **Metadata Fields and Metadata File.** Each of the metadata and coding fields set forth below that are readily available and can be extracted shall be produced for each document and electronically stored information. The parties are not obligated to populate manually any of the fields below if such fields cannot be extracted from a document or electronically stored information, with the exception of the following: BEGBATES, ENDBATES, BEGATTACH, ENDATTACH, CUSTODIAN, AND CONFIDENTIALITY. The metadata file shall be delimited according to the following characters:

- (i) Delimiter=~ (ASCII:020);
- (ii) Text-Qualifier= p (ASCII:254); and
- (iii) New Line=® (ASCII: 174).

Field Name	Field Description
BEGBATES	Beginning Bates number as stamped on the production image
ENDBATES	Ending Bates number as stamped on the production image
BEGATTACH	First production Bates number of the first document in a family
ENDATTACH	Last production Bates number of the last document in a family

Field Name	Field Description
HAS ATTACHMENTS	Indicates that an email has attachments
CUSTODIAN	The custodian of the document
PAGE COUNT	Total Number of pages in the document
OTHER_ CUSTODIAN	All individual(s) that had electronic files that were removed due to de-duplication (De-Duped Custodian) Field Name Field Description
DOCTYPE	The type of document (hardcopy) or electronic tile (e.g., Word, PDF, etc.) typically indicated by the file's extension
EXTENSION	Characters of the filename indicating the relevant portion used to open the file (file extension)
FULLPATH	The directory structure of the original file(s). Any container name is included in the path.
HASHVALUE	The MD5 or SHA-1 hash value
SUBJECT	Subject line of email
TITLE	Title from properties of document
DATESENT	Date email was sent (format: MM/DD/YYYY)
TIMESENT	Time email was sent
PARENT_DATE	The date of the parent email should be applied to the parent email and all of the email attachments
TO	All recipients that were included on the "To" line of the email
FROM	The name and email address of the sender of the email
CC	All recipients that were included on the "CC" line of the email
BCC	Recipient(s) of "blind carbon copies" of the email message
AUTHOR	Any value populated in the Author field of the document properties
FILENAME	Filename of an electronic document (Edoc or attachment)

Field Name	Field Description
DATEMOD	Date an electronic document was last modified (format: MM/DD/YYYY) (Edoc or attachment)
DATECREATED	Date the document was created (format: MM/DD/YYYY) (Edoc or attachment)
NATIVELINK	Native File Link (Native Files only)
CONFIDENTIALITY	The document confidentiality designation, if any

11. **Text Files.** A single multi-page text file shall be provided for each document or electronically stored information, and the filename should match the starting BEGBATES number of the document. A commercially acceptable technology for optical character recognition “OCR” shall be used for all scanned, hard copy documents. When possible, the text of native files should be extracted directly from the native file. Text files will not contain the redacted portions of the documents and OCR text files will be substituted instead of extracted text files for redacted documents.

12. **Image Load Files and Data Load Files.** Each TIFF in a production must be referenced in the corresponding image load file. The total number of documents referenced in a production’s data load file should match the total number of designated document breaks in the Image Load file(s) in the production. The total number of pages referenced in a production’s image load file should match the total number of TIFF files in the production. The total number of documents in a production should match the total number of records in the data load file.

13. **Bates Numbering.** All images must be assigned a unique Bates number that is sequential within a given document and across the production sets.

14. **Confidentiality Designation.** Responsive documents in TIFF format will be stamped with the appropriate confidentiality designations in accordance with the Confidentiality Order in this matter.

15. **Redaction of Information.** The producing party may redact from any TIFF image, metadata field, or native file material that is protected from disclosure by applicable privilege or immunity, contains information subject to the terms of the Confidentiality Order entered in this action, or is not responsive to a pending discovery request. In preparing families for production, the producing party also may redact entire attachments that are wholly non-responsive and may produce slipsheets in their place. Each redaction shall be indicated clearly. If documents are produced containing redacted information, an electronic copy of the original, unredacted data shall be securely preserved in such a manner so as to preserve without modification, alteration or addition the content of such data including any metadata therein.

16. **Native Format.** Electronic spreadsheets (e.g., Excel) or electronic presentations (e.g., PowerPoint), that have been identified as responsive and not privileged shall be produced in native format. The processed native for all such documents should be produced and linked to their corresponding documents by the metadata field "NATIVELINK." The requesting party may make reasonable requests for certain other electronic files and/or databases initially produced in their petrified (TIFF or PDF) format to be produced in their native format in the event that the petrified format is not reasonably usable. The requesting party shall identify the files or databases by their Bates numbers and the materials should be produced in their unaltered native format.

To the extent that a native file must be redacted, the producing party may redact either the native file or produce TIFF images with burned in redactions in lieu of a Native File and

TIFF placeholder image. If redacting TIFF images and to the extent that any of the following can be automated, the producing party, or its e-discovery vendor, should make reasonable efforts to: (1) reveal hidden cells prior to converting the document to TIFF; (2) clear any filters that may conceal information; (3) adjusts column widths so that numbers do not appear as “#####”; (4) ensures that column and row headings print; and (5) ensure that the tab name appears in the header or footer of the document. If, however, the end user has not designated a tab name to appear in the header or footer of the document, no additional undertaking will be required by the producing party, including no custom handling or manual interventions.

17. **Relational Databases and Database Management Systems.** The parties will meet and confer to attempt to agree upon the format of production by which discoverable electronically stored information in a relational database or database management system (e.g., Oracle, Access, SQL server, 082) can be produced.

18. **Email and attachments.** Email and attachments should be converted to single-page TIFF images and produced consistent with the specifications provided herein. Attachments shall be processed as separate documents, and the text database load file shall include a field in which the producing party shall identify the email and the specific attachment or attachments to which that email is related.

19. **Color Documents.** Except as otherwise specifically provided herein or agreed to by the parties, documents originally in color need not be produced in color unless the production in black and white alters or obscures the substance of the document. A party may make reasonable requests for documents or electronically stored information to be produced in a color format upon review of the other party’s production.

20. **Word Processing Files.** Word processing files, including without limitation Microsoft Word files (*.doc and * .docx), will be produced in the above TIFF format with tracked changes, comments, and hidden text showing.

21. **Dynamic Fields.** To the extent possible, files containing dynamic fields such as file names, dates, and times will be produced showing the field code (e.g., “[FILENAME]” or “[AUTODATE]”), rather than the values for such fields existing at the time the file is processed.

22. **Proprietary Files.** To the extent a response to discovery requires production of ESI accessible only through proprietary software, the parties should continue to preserve each version of such information. The parties shall meet and confer to finalize the appropriate production format.

23. **Embedded Files.** Except for signature blocks and non-substantive image files, embedded files must be treated as separate files. The load file shall include a field in which the producing party shall identify, for each document containing an embedded file, the production range of any such embedded file. This production range may be identified in the same field as the production range of an e-mail attachment.

24. **Compressed Files.** Compressed file types (i.e., .CAB, .GZ, .TAR .. z, .ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual files.

25. **Parent-Child Relationships.** Parent-Child relationships (the association between an attachment and its parent Document) must be preserved in such a way that a document or electronic file and any attachments are produced in the same production set and the relationships identifiable. The parties agree to provide beginning attachment and ending attachment fields in

the database load file to capture the entire production number range for the parent/child(ren) documents.

26. **Production Media.** Documents shall be produced on external hard drives, readily accessible computer(s), FTP sites, email or other electronic media (“Production Media”). Each piece of Production Media shall identify a production number corresponding to the production volume (e.g., “VOL001,” “VOL002”), as well as the volume of the material in that production (e.g., “-001,” “-002”). Each piece of Production Media shall also identify: (1) the producing party’s name; (2) the production date; and (3) the Bates Number range of the materials contained on the Production Media. To maximize the security of information in transit, any media on which documents or electronic files are produced may be encrypted by the producing party. In such cases, the producing party shall transmit the encryption key or password to the requesting party, under separate cover, contemporaneously with sending the encrypted media.

27. **Processing Exceptions.** The Parties agree that there is no need to preserve or collect ESI from the following sources, which are deemed to not likely contain relevant information and to be not reasonably accessible: audio or video files; voicemails; deleted, slack, fragmented, or other data only accessible with the use of forensic tools; random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system; online access data such as temporary internet files, history, cache, and cookies; backup data that is substantially duplicative of data that are more accessible elsewhere; text messages or SMS files; photograph files such as .jpg or .gif; mobile devices such as smart phones and tablets; server, system, or network logs; data remaining from systems no longer in use that are unintelligible on the systems in use; any file with a logical size of zero.

Furthermore, the Parties have agreed to engage in further meet-and-confer efforts regarding the preservation and collection of instant messages.